UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DISTRICT

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	No. 4:16-CR-258 CEJ (NAB)
	)	
ALDEN DICKERMAN,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE TO DEFENDANT’S MOTION FOR FRANKS HEARING

Comes now the United States of America, by and through its attorneys, Richard G. Callahan, United States Attorney for the Eastern District of Missouri, and Colleen Lang, Assistant United States Attorney for said district, and files its Response to Defendant’s Motion for a *Franks* hearing.

Defendant filed a motion and memorandum requesting a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). In support of his motion, defendant alleges that the affiant’s affidavit was inherently misleading and contained false statements and relevant omissions. As subsequently discussed in detail, these allegations are misplaced. Defendant fails to identify that any statements contained in the affidavits were deliberately or recklessly false. Nor does defendant show that omitted truthful statements, if supplemented in the affidavit, would have affected the probable cause determination. Accordingly, a showing has not been made to support a *Franks* hearing in this case.

I. FACTUAL BACKGROUND[1]

A. Background on Freenet and Law Enforcement Investigations on Freenet

In September of 2011, Special Investigator ("S.I.") Wayne Becker of the Dent County Sheriff's Department began to collect "keys" and files of child pornography located and being shared on "Freenet." In April of 2012, Special Investigator ("S.I.") Wayne Becker of the Dent County Sheriff's Department began to review logs for requests of files containing child pornography on Freenet in order to find individuals who were looking for and sharing child pornography on Freenet. Freenet is a type of peer-to-peer network software that allows users to share files over the Internet. It uses a decentralized, distributed data store to keep and deliver information. It is free and publicly available software for publishing and communicating on the Internet. Freenet's focus is to provide a place on the Internet for free speech and anonymity. In Freenet, each file is made up of several blocks, or splits, that are stored independently of each other. To view a file, you must request all the blocks that are necessary to reconstruct it. The keys used to identify a block to retrieve are the hash values of the blocks. Users contribute to the network by giving bandwidth and a portion of their hard drive for storing files. Freenet transmits data between nodes, also known as peers. Freenet also stores data on the nodes. The process of finding a piece of data, or a place to store data, is called routing. Nodes are the computers running Freenet. A node in Freenet interacts directly with its directly connected peers. Each peer's IP address is visible to a node, but a node does not learn the IP addresses of its peers' peers. On the current version of Freenet, a node may have up to 142 peers. (See Exhibit 1, "Statistical Detection of Downloaders of Child Exploitation Materials in Freenet" for more detail

[1] This factual background is identical to the factual background laid out in the Government's Response to Defendant's Motion to Suppress Evidence. The factual summary provided is intended as a general guide and is not intended as a comprehensive statement of the government's case.

on Freenet).

Researchers and law enforcement studied the Freenet open source code and analyzed activity on Freenet. Through their study they were able to create a statistical algorithm to determine the likelihood that a peer is the requestor of child pornography files, versus being a peer that only relayed the request. The timeline for these activities are as follows. Beginning in 2012, S.I. Becker collected keys in order to build database of files on Freenet that are associated with known or suspected child pornography images and videos. Researchers at the University of Massachusetts Amherst helped modify the Freenet program for law enforcement use. The modification logs the IP address, the content hash key values, the hops-to-live ("HTL"), types of requests, and the date/time of the requests as it passes through the node. Back in 2012 and 2013, this information was then collected by SI Becker's ICAC lab in Salem, Missouri. SI Becker analyzed that information to determine if the IP address appeared to be the likely requester of known child pornography files on Freenet.

SI Becker began investigating child pornography offenders on Freenet in 2012 and 2013. In 2014, the research staff at University of Massachusetts Amherst worked with SI Becker to develop a new method to determine if an IP address appeared to be requesting known child pornography files on Freenet.

In 2015, these researchers developed a statistical algorithm for determining whether a peer is more likely to be requesting child pornographic material on Freenet or relaying such a request. This algorithm was still being refined at the time of SI Becker's investigation into the defendant's requests for child pornography on Freenet. At the time of investigation into the defendant, SI Becker was using a method that is fundamentally similar to what the algorithm does now because both methods count requests for blocks that make up a file of known child pornography. A count of requests distinguishes the requesters from relayers.

While Freenet tries to be a harbor for anonymity, the website warns about the possibility that an IP address could be recognized. The website states, "If you are connected to a node, and can recognise the keys being requested (probably because it was posted publicly), you can show statistically that the node in question probably requested it, based on the proportion of the keys requested from that node, the locations of nearby nodes, the HTL on the requests and so on.[2]" The warning is basically what law enforcement is doing – recognizing known keys and determining whom is a requestor versus a relayer by the number of blocks being requested.

The mathematical algorithm that is currently in use for the law enforcement version of Freenet is laid out in further detail in the article, "Statistical Detection of Downloaders of Child Exploitation Materials in Freenet," and was written in July of 2016. Exhibit 1. The method the algorithm uses is very similar to the method that SI Becker used in 2015. The article sums up the algorithm as follows, "[b]riefly, the algorithm works by looking at the cumulative number of requests for blocks corresponding to a distinct file of interest made by any single node. It then calculates whether the number of requests observed is most likely what we would expect to observe if the peer were the originator of the request or just replaying request on behalf of other nodes." Ex. 1, page 4, section 4.

B. Instant Offense

While investigating Freenet requests on April 2, 2015, S.I. Becker came across a computer with an IP address in the state of Missouri that requested a file of known child

[2] Warning from the Freenet Project webpage (https://wiki.freenetproject.org/FAQ).

pornography. SI Becker documented the data related to that IP address' request for the file of child pornography on Freenet. Exhibit 2, SI Becker's Excel Spreadsheet. S.I. Becker collected the file and IP address information and sent it to Det. Michael Slaughter of the St. Louis County Police Department who sent a subpoena to AT&T Internet services to determine the subscriber information for that IP address. AT&T responded that the name and address of the subscriber was Janis Dickerman at 9524 Corregidor Drive, St. Louis, Missouri, 63134.

A computer search of the address revealed that Janis Dickerman had Ameren UE utilities in her name at that residence since 1959. A search warrant was prepared by Det. Slaughter and signed by St. Louis County Judge Borbonus on August 18, 2015. The search warrant stated "While reviewing requests received by undercover Freenet nodes, located in Missouri, SI Becker observed IP address 172.12.235.62 routing/or requesting suspected child pornography blocks. The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requestor of the file." Exhibit 3, Search Warrant Affidavit, ¶ 6. "SI Becker observed that on April 2, 2015, between 11:08 p.m. UTC and 11:10 p.m. UTC a computer running Freenet software, at IP address 172.12.235.62, requested from Freenet law enforcement nodes 69 parts, or blocks, of the following file." Ex. 3, ¶ 7. The affiant then identified that file with its' name and unique SHA1 hash value. The file was then described as a folder containing seventeen (17) images of a young prepubescent child in a lascivious display of her genitals and being anally penetrated. In paragraphs twelve (12) through twenty-two (22) of the search warrant affidavit, Freenet was described and explained at length. Ex. 3.

The search warrant was executed by St. Louis County Police on August 18, 2015, at 9524 Corregidor Drive, St. Louis, Missouri. The defendant, Alden Dickerman, was the only person home during the execution of the warrant. After being read his *Miranda* warnings, the defendant told police that he lived in the home with his mother (Janis Dickerman) and his sister. The defendant stated that he owned three computers including a laptop. He stated that he was only user of his laptop, which was password protected. Further, the defendant told Det. Slaughter that he had used Freenet software. When asked about downloading pornography from Freenet, the defendant asked for an attorney and questioning about the case ceased.

Meanwhile Det. Partney and S.I. Becker searched the home for computers and computer-related devices. They previewed the defendant's computers at the residence to see if they contained child pornography. These computers were located in the defendant's bedroom. Two of the defendant's computers did not contain child pornography. A third computer belonging to the defendant was an Asus laptop computer that was password protected. Detectives located a typed list of passwords in the defendant's bedroom and were able to use one of the passwords to access the Asus laptop. S.I. Becker determined the Asus laptop contained Freenet software and files of child pornography.

On August 21, 2015, S.I. Becker began a forensic review of the Asus laptop. S.I. Becker is a qualified forensic examiner. S.I. Becker located 597 images of child pornography and 43 videos of child pornography on the defendant's laptop computer's Hitachi hard drive. Freenet and the related Frost software were also located on the laptop. Frost is a group message board that relies on the Freenet peer-to-peer network. S.I. Becker also found that the defendant was subscribed to three boards on Frost, "pthc," "lolicam," and "hurtcore." The titles of the boards are indicative of child pornography. Many of the images and videos found on the laptop depicted prepubescent minor children, under the age of twelve, engaging in sexually explicit conduct. S.I. Becker noted that about thirty-two (32) of the images and nine (9) of the videos depicted the sex abuse of children as young as toddlers or infants. Many of the images and videos also portrayed sadistic or masochistic conduct.

On June 22, 2016, a federal grand jury indicted the defendant on one count of Possession of Child Pornography in violation of Title 18 U.S.C. Section 2252(a)(5)(B).

II. LEGAL ANALYSIS

A *Franks* hearing should not be granted unless there is actual evidence that the search warrant was invalid.

> "There is, of course, a presumption of validity with respect to the affidavit supporting the search warrant. To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof." *Franks v. Delaware*, 438 U.S. 154, 171 (1978).

The defendant has raised mere allegations in his motion that the affiant misrepresented the accuracy of his findings in the search warrant. The defendant has not provided factual evidence or data to back up these assertions. The defense has failed to meet its burden to prove that the presumed valid affidavit in support of the warrant was actually invalid.

It is well established that "to obtain relief under *Franks*, 'a defendant must first demonstrate that the law enforcement official deliberately or recklessly included a false statement, or omitted a truthful statement from his warrant affidavit." *United States vs Mashek,* 606 F.3d 922, 928 (8th Cir.2010). see also *United States v. McIntryre*, 646 F.3d 1107, 1113-14 (8th Cir.2011)(quoting *Mashek*). Furthermore, before a defendant may receive such a hearing, the reviewing magistrate judge must determine that the allegedly false statement was necessary to the finding of probable cause. *Franks v. Delaware*, 438 U.S. 154 (1978); see also *United States v. Mashek*, 606 F.3d 922, 928 (8th Cir.2010)(citing *United States v. Reinhollz*, 245 F.3d 765, 774 (8th Cir.2001); *United States v. Jansen*, 470F.3d 762, 765-66 (8th Cir. 2006); *United*

States vs. Sandoval-Rodriguez, 452 F,3d 984,988 (8th Cir. 2006).

"Allegations of negligence or innocent mistake will not suffice to demonstrate a recklessness or deliberate falsehood." *Mashek*, 660 F.3d at 928 (citing *Franks*, 438 U.S. at 171). "In determining if 'an affiant's statements were made with a reckless disregard for the truth,' the test is whether, after viewing all the evidence, that affiant must have entertained serious doubts as to the truth of his statement or had obvious reasons to doubt the accuracy of the information he reported.'" *McIntyre*, 646 F.3d at 1114 (quoting *United States v. Butler*, 594 F.3d 955, 961 (8th Cir. 2010). "A showing of deliberate or reckless falsehood is not lightly met." *Id.*

The defendant has not met his burden with regard to either prong of *Franks*. A *Franks* hearing should not be granted unless there is actual evidence that the search warrant was invalid. The search warrant is valid on its' face. With respect to the allegation that Detective Slaughter's affidavit was inherently misleading and contained false statements, defendant never proves how the statement is false. The defendant writes in their motion that the following statement from the search warrant affidavit was a false representation of the findings of SI Becker's investigation, "[t]he number and timing of the requests was significant enough to indicate that the IP address was the apparent original requester of the file." Defendant alleges that the significant number and timing of the requests could not have been apparent unless SI Becker independently verified the assumptions. SI Becker did verify the number and timing of the requests by tracking them in an Excel spreadsheet. Ex 2. This spreadsheet has been provided to the defendant along with two articles regarding how Freenet works. The number and timing of the requests was significant enough to determine the defendant was the requestor of the file. While using a law enforcement version of Freenet modified to passively log observations, SI Becker could observe the streams of data coming through Freenet from the defendant's IP address. This significant data logged included information such as the time and frequency of requests for certain files of interest from a node. Ex. 2. SI Becker then reviewed the significant data and calculate the percentage of even share. Ex. 2. The higher the percentage of even share and the more requests per second there are for a file of interest – the more likely the requests are coming from the requestor and not a forwarder. Ex. 1, Section 3 and Ex. 2. The defendant requested a file of interest titled, "April – Another Set 2 (set 2).zip," on Freenet. Within 1 minute and 58 seconds the defendant requested the multiple blocks that together will make up the file. The law enforcement node, "LE #693," received 69 requests for that file that when complete contains 783 data blocks. Thus, 8.81% of the minimum necessary requests went through the law enforcement node on Freenet from the defendant's IP address. The defendant had an average of 56.9 peers during the period of investigation (which includes the law enforcement node). On average, each peer would expect to receive an even proportion (i.e. share) of requests. If the defendant had been a relayer rather than a requestor, the law enforcement node would have received a much smaller percentage of the requests. The process was repeated three times for three separate files on three separate days. Ex. 2. SI Becker did verify the conclusion "that requests were significant enough," and kept track of this verification in his notes. Therefore, the statement in the affidavit is not false, but true because it is the correct conclusion to be drawn from SI Becker's investigation of the defendant on Freenet.

The defendant goes to assert that above quoted statement from the search warrant is a false representation because it *omits* that SI Becker independently verified his conclusions. SI Becker did verify the conclusion "that requests were significant enough" as detailed in the paragraph above. While this analysis performed by SI Becker was not in the search warrant, only the conclusion of it, that does not make the search warrant misleading. Not every detail of an investigation needs to be contained in the search warrant. Omissions to the search warrant are different then misrepresentations and require a different two-step test. The defense "must prove first that facts were omitted with the intent to make, or in reckless disregard of whether they make, the affidavit misleading, and, second, that the affidavit, if supplemented by the omitted information, could not support a finding of probable cause." *United States v. Allen*, 297 F.3d 790, 795 (8th Cir. 2002).

By supplementing the missing information into the search warrant, namely that SI Becker kept track of the probability of number and timings of the requests from defendant's IP address on Freenet, it actually bolsters the probable cause for the search warrant, not decreases it. Further, the information is not misleading since it is does not lead to a result other than the one described in the search warrant. The search warrant affidavit describes in paragraphs twelve (12) through twenty-two (22) how Freenet works. Ex. 3.

Defendant next argues that Detective Slaughter's omission of the behavior of Freenet's routing necessary to estimate the probability that the received requests originated from the peer they were received from (instead of forwarded form elsewhere) is based in part on how many requests are received. Defendant asserts that the routing behavior and how it was working on a particular day could affect the interpretation of the results. Defendant goes on to then allege that a potential for false positives was also omitted from the search warrant affidavit. In response, the routing was working correctly on April 2, 2015. SI Becker knows from his extensive experience on Freenet and how it works, that the routing and bandwidth had to have been working properly for several reasons. First, the defendant had an average of 59.6 peers on Freenet at the time of the request for the file titled, "April – Another Set 2 (set 2).zip." The minimum number of peers on Freenet is ten peers. To have as many as 59.6 peers, as the defendant did, the routing and bandwidth was working properly. Second, the timing of the blocks being received by the defendant after he requested them is significant. The requests for the blocks that make up the file were sent by the defendant were logged at being within one minute and fifty-eight seconds. Once the file is requested, Freenet locates blocks that make up the file on different nodes on Freenet. The blocks are then sent to the requestor and once the minimum number of blocks needed to create the file are received, then the file can then be downloaded by the requestor. Based on SI Becker's experience on Freenet, if the bandwidth was poor then the defendant would have had much less peers, closer to 10 or lower, and would not have requested the blocks of the file so quickly.

Third, the defendant alleges there is a potential for false positives that might have resulted and that should have been in the search warrant affidavit. In this case, false positives did not result. No false positive rate has been established for the exact method SI Becker was using in 2015, however, that method is very similar to the one documented in Ex. 1. In July of 2016, a false positive rate was estimated by the researchers from University of Massachusetts at Amherst for the method described in Exhibit 1. In a test sampling four months of data, they observed a false positive rate of 1.35%. Plus, in this case, both Freenet and child pornography files were located on the defendant's computer during the execution of the search warrant – confirming that the search warrant was not based on a false positive result. Further, SI Becker saw that the defendant's IP address requested and received child pornography files on Freenet on June 6, 2015, and June 13, 2015. Since defendant's IP address was seen downloading two more files of child pornography in June of 2015, the likelihood that the defendant's April 2, 2015 was a false positive or based on poor bandwidth is even more reduced. Ex. 2. The defendant makes a blanket statement not supported by any facts, that "false positives are likely to occur."

Steve Dougherty's affidavit is not sufficient to mandate an evidentiary hearing under *Franks*. The defense expert's affidavit never specifically points out that SI Becker's conclusions or analysis was incorrect. The defense expert, Steve Dougherty, states that the law enforcement modified version of Freenet "uses a large list of suspected illegal files and the behavior of Freenet's routing to estimate the probability that received requests originated from the peer they were received from instead of forwarded through the peer from a different one, based in part on how many requests are received from the peer relative to the file's total size." Defendant's Ex. B ¶ 11. "For the attack's estimation to be accurate, routing must be working well between the peers at that particular time." Defendant's Ex. B ¶12. Nowhere does Mr. Dougherty claim that the routings were not working effectively at that time of SI Becker's investigations. Further, as detailed above, SI Becker could tell from looking at the streams of data, the number of peers the defendant had, the frequency of the blocks being received, and the timing of file being received by the defendant, that the routing and bandwidth were working correctly.

There are no false statements in the search warrant affidavit. The omissions, which are basically the raw data backing up SI Becker's ultimate conclusions, only bolsters the probable cause when supplementing. Neither prong of the *Franks* test has been met and, therefore, the defendant is not entitled to a *Franks* hearing.

III. <u>CONCLUSION</u>

In conclusion, defendant fails to establish that any of the statements in the affidavit are deliberately false or made in reckless disregard for the truth. A *Franks* hearing should not be granted unless there is actual evidence that the search warrant was invalid. The search warrant is valid and there is no evidence otherwise. The omissions from the search warrant affiant would not change the probable cause basis for the issuance of the search warrant once supplemented into the affidavit. The affidavit of Steve Dougherty submitted by the defendant also does not prove which statements in the affidavit are deliberately false or made with reckless disregard for the truth. The defendant has not met his burden of establishing the need for a *Franks* hearing. The defendant has not shown *any* falsehood nor any material or significant omission from the search warrant affidavit. Wherefore, the government respectfully requests this Court to overrule and deny defendant's motion for a *Franks* hearing.

Respectfully submitted,

RICHARD G. CALLAHAN
United States Attorney

s/ Colleen Lang
Colleen Lang, #56872MO
Assistant United States Attorney
111 South 10th Street, Room 20.333
St. Louis, MO 63102
(314) 539-2200

CERTIFICATE OF SERVICE

I hereby certify that on November 21, 2016, the foregoing was filed electronically with the Clerk of the Court. The foregoing was emailed to all counsel of record by the undersigned.

s/ Colleen Lang
Colleen Lang, #56872MO
Assistant United States Attorney